IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. 10/801,332
Filing Date ..... March 15, 2004
Inventor..... Rudolph Balaz et al.
Group Art Unit 2131
Examiner ..... Revak, Christopher A.
Attorney's Docket No. MS1-467USC2
Confirmation No. 1955
Title: VPN Enrollment Protocol Gateway

APPEAL BRIEF

To: Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

From: Allan Sponseller (Tel. 509-324-9256x215; Fax 509-323-8979)
Customer No. 22801

Pursuant to 37 C.F.R. §41.37, Applicant hereby submits an appeal brief for application 10/801,332 within the requisite time from the date of filing the Notice of Appeal. Accordingly, Applicant appeals to the Board of Patent Appeals and Interferences seeking review of the Examiner's rejections.

(1) Real Party in Interest

The real party in interest is Microsoft Corporation, the assignee of all right, title and interest in and to the subject invention.

(2) Related Appeals and Interferences

Appellant is not aware of any other appeals, interferences, or judicial proceedings which will directly affect, be directly affected by, or otherwise have a bearing on the Board's decision to this pending appeal.

(3) Status of Claims

Claims 1-5 and 7-21 stand rejected and are pending in this Application. Claims 1-5 and 7-21 are appealed. Claims 1, 10, and 19 were previously amended. Claim 6 was previously canceled. Claims 1-5 and 7-21 are set forth in the Appendix of Appealed Claims on page 15.

(4) Status of Amendments

A Final Office Action was issued on May 16, 2005.

A Response to the Final Office Action was filed June 22, 2005. No amendments were made as part of this Response.

An Advisory Action was issued on July 7, 2005.

A Notice of Appeal was filed on August 15, 2005 in response to the Final Office Action and the Advisory Action.

An Office Action reopening prosecution was issued on April 5, 2006.

A Notice of Appeal was filed on August 7, 2006.

(5) Summary of Claimed Subject Matter

A concise explanation of each of the independent claims is included in this Summary section, including specific reference characters. These specific reference characters are examples of particular elements of the drawings for certain embodiments of the claimed invention, and the claims are not limited to solely the elements corresponding to these reference characters.

With respect to independent claim 1, as discussed for example at page 12, line 24 through page 15, line 19, page 17, lines 7-15, and page 28, line 23 through page 30, line 23, a method, implemented in a registration authority, comprises receiving (430) a request, from a requestor, for a password to be used by a device when communicating with the registration authority operating as a protocol gateway between the device and a certificate authority. The method further comprises authenticating (432) the requestor, generating (438) the password, adding (438) the password to a password table, and returning (440) the password to the requestor for use by the device.

With respect to independent claim 10, as discussed for example at page 12, line 24 through page 15, line 19, page 17, lines 7-15, and page 28, line 23 through page 30, line 23, one or more computer-readable media having stored thereon a plurality of instructions that implement a registration authority and that, when executed by one or more processors, causes the one or more processors to perform acts comprising receiving (430) a request, from a requestor, for a password to be used by a device when communicating with the registration authority operating as a protocol gateway between the device and a certificate authority. The acts further comprise authenticating (432) the requestor, generating (438) the password,

adding (438) the password to a password table, and returning (440) the password to the requestor for use by the device.

With respect to independent claim 19, as discussed for example at page 12, line 24 through page 15, line 19, page 17, lines 7-15, and page 28, line 23 through page 30, line 23, a registration authority system comprises means for receiving a request (drawings: 430, 142, 172, 174; specification: p. 29, lines 6-16, p. 9, line 11 – p. 18, line 4, p. 7, lines 9-12, and p. 31, lines 8-12), from a requestor, for a password to be used by a device when communicating with the registration authority operating as a protocol gateway between the device and a certificate authority. The system further comprises means for authenticating (drawings: 432, 142, 172, 174; specification: p. 29, lines 6-10, p. 29, lines 16-18, p. 9, line 11 – p. 18, line 4, p. 7, lines 9-12, and p. 31, lines 8-12) the requestor, means for generating (drawings: 438, 142, 172, 174; specification: p. 29, lines 6-10, p. 29, line 22 – p. 30, line 4, p. 9, line 11 – p. 18, line 4, p. 7, lines 9-12, and p. 31, lines 8-12) the password, means for adding (drawings: 438, 142, 172, 174; specification: p. 29, lines 6-10, p. 29, line 22 – p. 30, line 8, p. 9, line 11 – p. 18, line 4, p. 7, lines 9-12, and p. 31, lines 8-12) the password to a password table, and means for returning (drawings: 440, 142, 172, 174; specification: p. 29, lines 6-10, p. 30, lines 9-11, p. 9, line 11 – p. 18, line 4, p. 7, lines 9-12, and p. 31, lines 8-12) the password to the requestor for use by the device.

(6) Grounds of Rejection to be Reviewed on Appeal

Claims 1-5 and 7-20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,044,471 to Colvin in view of U.S. Patent

No. 6,606,744 to Mikurak. Appellant respectfully submits that claims 1-5 and 7-20 are not obvious over Colvin in view of Mikurak.

Claim 21 stands rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,044,471 to Colvin in view of U.S. Patent No. 6,606,744 to Mikurak and further in view of U.S. Patent No. 6,931,016 to Andersson et al. Appellant respectfully submits that claim 21 is not obvious over Colvin in view of Mikurak and further in view of Andersson.

(7) Argument

A. Rejection under 35 U.S.C. §103(a) over U.S. Patent No. 6,044,471 to Colvin in view of U.S. Patent No. 6,606,744 to Mikurak.

Claims 1-5 and 7-20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,044,471 to Colvin (hereinafter "Colvin") in view of U.S. Patent No. 6,606,744 to Mikurak (hereinafter "Mikurak").

Colvin is directed to a method and apparatus for securing software to reduce unauthorized use (see, title). As discussed in Colvin, each copy or group of copies of software is associated with a password (see, col. 3, lines 59-63). During the initial use or installation of the software on a computer, the end user must contact a password administrator to obtain the appropriate authorization code or password (see, col. 4, lines 33-39). The password administrator obtains registration information from the end user and provides an appropriate password or authorization code to the software (see, col. 4, lines 39-42). The password administrator stores the registration information to be used for various purposes to reduce unauthorized use of software (see, col. 4, line 66 to col. 5, line 2). The

password or authorization code is communicated to the software to make the software operational on the end user's computer (see, col. 6, lines 38-40).

Mikurak is directed to collaborative installation management in a network-based supply chain environment (see, col. 1, lines 9-10). As discussed in the Abstract of Mikurak, telephone calls, data and other multimedia information are routed through a network system which includes transfer of information across the internet utilizing telephony routing information and internet protocol address information. The system includes integrated Internet Protocol (IP) telephony services allowing a user of a web application to communicate in an audio fashion in-band without having to pick up another telephone. Users can click a button and go to a call center through the network using IP telephony. The system invokes an IP telephony session simultaneously with the data session, and uses an active directory lookup whenever a user uses the system. Users include service providers and manufacturers utilizing the network-based supply chain environment.

1. Claims 1-5 and 7-20

In the April 5, 2006 Office Action at p. 4-5, ¶2, it was asserted that, with respect to claims 1, 10, and 19:

> It is disclosed by Mikurak of a registration authority that acts as a protocol gateway that is coupled to receive messages from a certificate authority (col. 67, lines 15-19, 21-25, col. 269, lines 58-65, and as shown in Figure 120). . . . Mikurak recites motivation for the use of a registration authority acting as a protocol gateway by disclosing without the use of gateways to convert the protocols, the transmitted information would be incomprehensible upon arrival and gateways allow incompatible networks to communicate with one another (col. 67, lines 15-25).

Appellant respectfully disagrees with this characterization of Mikurak. Mikurak, at col. 67, lines 15-25 recites:

> In terms of architecture, two given networks are connected by a computer that attaches to both of them. Internet gateways and routers provide those links necessary to send packets between networks and thus make connections possible. Without these links, data communication through the Internet would not be possible, as the information either would not reach its destination or would be incomprehensible upon arrival. A gateway may be thought of as an entrance to a communications network that performs code and protocol conversion between two otherwise incompatible networks. For instance, gateways transfer electronic mail and data files between networks over the internet.

Furthermore, Mikurak at col. 269, lines 58-65 recites:

> The central corporate headquarters will maintain a CA (Certificate Authority) to administer the certificates. The CA is integrated with an LDAP server to store directory information. An RA (Registration Authority) is used to process certificate requests. For users at customer locations, the authentication occurs at the corporate web server and is managed by the web server access control software.

As can be seen from the cited portions of Mikurak, although Mikurak discusses Internet gateways and also discusses a Certificate Authority and a Registration Authority, there is no mention or discussion of a Registration Authority operating as a protocol gateway between a device and a Certificate Authority. The Internet gateway and Registration Authority of Mikurak are described as separate devices – there is no discussion or mention in Mikurak of including the functionality of the Internet gateway in the Registration Authority of Mikurak. The discussion of an Internet gateway in Mikurak to perform code and protocol conversion between two otherwise incompatible networks does not provide any suggestion to include the functionality of the Internet gateway in the Registration Authority. Appellant

respectfully submits that the mere existence of another device on the network does not make it obvious to incorporate the functionality of that device into the Registration Authority of Mikurak. As such, Appellant respectfully submits that Mikurak does not disclose or suggest the registration authority operating as a protocol gateway between the device and a certificate authority as recited in claims 1, 10, and 19.

In the April 5, 2006 Office Action at pp. 2-3, ¶ 2, it was also asserted that:

> Protocol gateways are notoriously well known to one of ordinary skill in the art as be responsible for convert the protocols, the transmitted information would be incomprehensible upon arrival and gateways allow incompatible networks to communicate with one another, see Mikurak col. 67, lines 15-25. The protocol gateway operates through the Internet which is connected between the registration authority, device, and certificate authority, see Mikurak col. 67, lines 15-25 and Figure 120.

Appellant respectfully submits, however, that Mikurak does not disclose a registration authority operating as a protocol gateway as recited in claims 1, 10, and 19. Mikurak at col. 67, lines 15-25 discusses gateways that make connections between two networks possible, and that perform code and protocol conversion between two otherwise incompatible networks. Additionally, Mikurak at col. 269, lines 58-65 discusses that the Registration Authority is used to process certificate requests. However, nowhere in the cited portion of Mikurak, or elsewhere in Mikurak, is there any discussion or mention of using a Registration Authority as a protocol gateway or of why one would want to use a Registration Authority as a protocol gateway. The Internet Gateway and the Registration Authority of Mikurak are described as separate devices. Appellant respectfully submits that there is no discussion or mention in Mikurak of the Registration Authority

operating as an Internet gateway, or of the Registration Authority incorporating the functionality of an Internet gateway. Without any such discussion or mention, Appellant respectfully submits that Mikurak cannot disclose or suggest the registration authority operating as a protocol gateway between the device and a certificate authority as recited in claims 1, 10, and 19.

With respect to Colvin, Colvin is not cited as curing and does not cure these deficiencies of Mikurak.

For at least these reasons, Appellant respectfully submits that claims 1, 10, and 19 are allowable over Colvin in view of Mikurak.

Given that claims 2-5 and 7-9 depend from claim 1, claims 11-18 depend from claim 10, and claim 20 depends from claim 19, Appellant respectfully submits that claims 2-5, 7-9, 11-18, and 20 are likewise allowable over Colvin in view of Mikurak for at least the reasons discussed above.

B. Rejection under 35 U.S.C. §103(a) over U.S. Patent No. 6,044,471 to Colvin in view of U.S. Patent No. 6,606,744 to Mikurak and further in view of U.S. Patent No. 6,931,016 to Andersson et al.

Claim 21 stands rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,044,471 to Colvin (hereinafter "Colvin") in view of U.S. Patent No. 6,606,744 to Mikurak (hereinafter "Mikurak") and further in view of U.S. Patent No. 6,931,016 to Andersson et al. (hereinafter "Andersson").

Andersson is directed to a virtual private network management system (see, Title). As discussed in the Abstract of Andersson, a request to join the virtual private network is received from a given network device having a given network

device identifier that identifies the given network device. The set of network device identifiers then is retrieved from the network device memory set to identify all network devices in the set of network devices. A notify message then is forwarded to each of the set of network devices, and a join message is forwarded to the given network device. The notify message includes the given network device identifier, while the join message includes the set of network device identifiers. The given network device identifier then is stored in the network device memory set.

1. Claim 21

With respect to claim 21, claim 21 depends from claim 1 and Appellant respectfully submits that claim 21 is allowable over Colvin in view of Mikurak due to its dependency from claim 1. With respect to Andersson, Andersson is not cited as curing and does not cure the deficiencies of Colvin in view of Mikurak discussed above. Accordingly, Appellant respectfully submits that claim 21 is allowable over Colvin in view of Mikurak and further in view of Andersson.

Furthermore, claim 21 recites:

> A method as recited in claim 1, further comprising:
> receiving the password as part of a subsequent request from the device; and
> comparing the received password to the password in the password table to verify that the subsequent request actually came from the device.

Appellant respectfully submits that no such receiving and comparing is disclosed or suggested by Colvin in view of Mikurak and further in view of Andersson.

In the April 5, 2006 Office Action at p. 7, ¶ 3, it was asserted that:

> It is taught by Andersson et al of receiving a password as part of a subsequent request from the device and comparing the received password to the password in the password table to verify that the subsequent request actually came from the device (col. 3, line 67 through col. 4, line 6 and col. 4, lines 18-27).

Appellant respectfully disagrees with this characterization of Andersson. Andersson, at col. 3, line 67 – col. 4, line 6 recites:

> Each VPN has an associated VPN identification code, security data relating to the VPN, and a list of network devices (i.e., routes 18) that are members of the specified VPN. Among other things, the security data may include authentication data for authenticating routers 18 attempting to access the VPN, such as encryption keys an/or passwords.

Further, at col. 4, lines 10-26 Andersson recites:

> The process begins at step 400 in which a request message from a router 18 attempting to join a given VPN is received at the input port 28 of the manager server 14. . . . Upon receipt of the request, the VPN logic 26 parses the request to determine the VPN identifier, IP address, and the security data (step 402). The VPN logic 26 then determines, at step 404, if the router 18 is permitted to join the VPN to which membership is requested. To that end, the VPN logic 26 may access the database 22a to determine if the security data in the request matches the security data in the database 22a. For example, a password may be compared to determine if access to the VPN is permitted.

Thus, it can be seen from these cited portions of Andersson that the passwords discussed in Andersson are for the entire VPN, not for a single router in the VPN. The passwords discussed in Andersson can be used to verify that a router is permitted to join a VPN, but nowhere in Andersson is there any discussion or mention that the passwords can be used to verify that a particular request came from a particular router. Appellant respectfully submits that

nowhere in Andersson is there any disclosure or suggestion of a password being used to verify that a request actually came from a particular device.

Andersson further discusses at col. 4, lines 44-52 that a new database may be initialized if a request is received for a VPN that is not currently executing, that the new database may include security data parsed from the request, and that the security data parsed from the request is utilized to authenticate subsequent network devices attempting to access the noted VPN. This security data, as discussed above, would include the password of Andersson. If this security data (including the password) is to be used to authenticate subsequent network devices attempting to access the VPN, then the password must be for all devices in the VPN rather than for a specific device (if the password were for a specific device, how could the password received from one device be used to authenticate another device?). Thus, Appellant respectfully submits that a password of Andersson is for all devices in the VPN, not for a specific device.

Accordingly, Appellant respectfully submits that Andersson cannot disclose comparing the received password to the password in the password table to verify that the subsequent request actually came from the device as recited in claim 21. With respect to Colvin and Mikurak, Appellant respectfully submits that Colvin and Mikurak are not cited as curing, and do not cure, these deficiencies of Andersson.

For at least these reasons, Appellant respectfully submits that claim 21 is allowable over Colvin in view of Mikurak and further in view of Andersson.

Conclusion

The Office's basis and supporting rationale for the § 103(a) rejections is not supported by the teaching of the cited references. Appellant respectfully requests that the rejections be overturned and that pending claims 1-5 and 7-21 be allowed to issue.

Respectfully Submitted,

Dated: January 5, 2007

By: /Allan T. Sponseller/
Allan T. Sponseller
Lee & Hayes, PLLC
Reg. No. 38,318
(509) 324-9256 ext. 215

(8) Appendix of Appealed Claims

1. (Previously presented) A method, implemented in a registration authority, comprising:

receiving a request, from a requestor, for a password to be used by a device when communicating with the registration authority operating as a protocol gateway between the device and a certificate authority;

authenticating the requestor;

generating the password;

adding the password to a password table; and

returning the password to the requestor for use by the device.

2. (Original) A method as recited in claim 1, wherein the device comprises a router.

3. (Original) A method as recited in claim 1, wherein generating the password comprises generating a random number as the password.

4. (Original) A method as recited in claim 1, wherein receiving, authenticating, and returning include using Secure Sockets Layer (SSL) to maintain secure communication with the device.

5. (Original) A method as recited in claim 1, further comprising keeping the password active for a selected amount of time.

7. (Original) A method as recited in claim 5, wherein keeping the password active for a selected amount of time comprises removing the password from the password table after the selected amount of time.

8. (Original) A method as recited in claim 1, further comprising:

receiving a request from the device, the request including a request password;

checking whether the request password is included in the password table; and

processing the request if the request password is included in the password table, otherwise rejecting the request.

9. (Original) A method as recited in claim 8, further comprising removing, if the request password is included in the password table, the request password from the password table.

10. (Previously presented) One or more computer-readable media having stored thereon a plurality of instructions that implement a registration authority and that, when executed by one or more processors, causes the one or more processors to perform acts comprising:

receiving a request, from a requestor, for a password to be used by a device when communicating with the registration authority operating as a protocol gateway between the device and a certificate authority;

authenticating the requestor;

generating the password;

adding the password to a password table; and

returning the password to the requestor for use by the device.

11. (Original) One or more computer-readable media as recited in claim 10, wherein the device comprises a router.

12. (Original) One or more computer-readable media as recited in claim 10, wherein generating the password comprises generating a random number as the password.

13. (Original) One or more computer-readable media as recited in claim 10, wherein receiving, authenticating, and returning include using Secure Sockets Layer (SSL) to maintain secure communication with the device.

14. (Original) One or more computer-readable media as recited in claim 10, wherein the plurality of instructions further cause the one or more processors to perform acts comprising keeping the password active for a selected amount of time.

15. (Original) One or more computer-readable media as recited in claim 14, wherein keeping the password active for a selected amount of time comprises marking the password as invalid after the selected amount of time.

16. (Original) One or more computer-readable media as recited in claim 14, wherein keeping the password active for a selected amount of time comprises removing the password from the password table after the selected amount of time.

17. (Original) One or more computer-readable media as recited in claim 10, wherein the plurality of instructions further cause the one or more processors to perform acts comprising:

receiving a request from the device, the request including a request password;

checking whether the request password is included in the password table; and

processing the request if the request password is included in the password table, otherwise rejecting the request.

18. (Original) One or more computer-readable media as recited in claim 17, wherein the plurality of instructions further cause the one or more processors to perform acts comprising removing, if the request password is included in the password table, the request password from the password table.

19. (Previously presented) A registration authority system comprising:

means for receiving a request, from a requestor, for a password to be used by a device when communicating with the registration authority operating as a protocol gateway between the device and a certificate authority;

means for authenticating the requestor;

means for generating the password;

means for adding the password to a password table; and

means for returning the password to the requestor for use by the device.

20. (Original) A system as recited in claim 19, wherein the device comprises a router.

21. (Previously presented) A method as recited in claim 1, further comprising:

receiving the password as part of a subsequent request from the device; and

comparing the received password to the password in the password table to verify that the subsequent request actually came from the device.

(9) Appendix of Evidence Submitted

None.

(10) Appendix of Related Proceedings

None.